The Trusted Insider:

How Espionage Feeds the Chinese Economy

By: Rachel M. Houhoulis and Eric M. O'Neill

THE GEORGETOWNGROUP™
STATE OF THE ART INTELLIGENCE

Castle Advisory Group

Executive Summary

Robert Hanssen, a senior FBI Agent was convicted of espionage after spying for the Soviet Union and Russia for over twenty years. In his lengthy career as Russia's top spy, Hanssen systematically compromised the United States ability to conduct counterintelligence, providing "ways and means" information on how the U.S. performs national counterintelligence operations, information related to foreign assets, and information that compromised undercover operations. Hanssen also revealed information related to the U.S. nuclear arsenal and provided contingency of government plans for a nuclear attack and dropped information that led to the deaths of United States intelligence assets. Hanssen has been called the most damaging spy in United States history and his actions highlight a key example of the extensive damage a trusted insider can create for an organization, even one so security focused as the FBI.

Recently Edward Snowden, a contract analyst for the NSA, admitted to stealing hundreds of thousands of highly classified files detailing U.S. intelligence collection programs by the NSA. The NSA estimates up to 1.7 million classified files may have been stolen. The information leak by Snowden has been characterized as one of the most damaging in history and, according to the Director of National Intelligence, has compromised critical foreign intelligence collection sources. After stealing the documents, Snowden fled to Hong Kong in the People's Republic of China (PRC) and then Russia, where he has since remained under an asylum plea. Operationally, the U.S. Intelligence Community must now assume that all information stolen by Snowden has been collected by the Chinese and Russians, not just the information which has been published. Snowden is currently wanted by the U.S. on charges of theft of U.S. government property and espionage.

Snowden's security breaches mirror the significant damage caused by Hanssen in at least one respect. Both insiders revealed information that compromised the ability of their respective agencies to function, costing significant time and money in review procedures and requiring years of diligence to assess the extent of the damages and correct the harm. Snowden and Hanssen had different motivations for turning traitor and their reasons for doing so continue to be debated by the Intelligence Community. Ultimately, however, the "why" does not matter in light of the profound damage each caused to their respective agencies, the larger Intelligence Community and to United States counterintelligence goals.

On May 1, 2014, the Justice Department indicted five members of the Chinese military on charges of hacking into computers and stealing valuable trade secrets from U.S. nuclear, solar and steel companies. The indictment charges five individuals in the People's Liberation Army (PLA) with computer fraud, conspiracy to commit computer fraud, damaging a computer, aggravated identity theft and economic espionage. Information stolen by the PLA from five leading U.S. companies included thousands of files containing cost and pricing information, production information that could help a competitor shorten its research and development timeline and other information geared to provide a competitive advantage to Chinese industry.

The most critical asset of any organization is intellectual property. Unfortunately, this value is recognized by people, competitors and other nation states, making intellectual property and technology a top target for economic and industrial espionage. As stated by the former Commander of the United States Cyber Command and Director of the National Security Agency, General (retired) Keith Alexander, the ongoing theft of IP is “the greatest transfer of wealth in history.” The greatest threat to robust security measures that protect this information is often the trusted insider - the Robert Hanssen or Edward Snowden - that is able to exploit information from within the company firewall. When it comes to the PRC, economic espionage is a powerful economic development tool. In the PRC, international businesses need to protect themselves not just from other firms, but from the state apparatus itself.

This white paper analyzes current trends and concerns in economic espionage by the trusted insider with a particular focus on the PRC’s intelligence collection goals.

Contents

China's Economic Growth is Tied to Spy Craft

The PRC's economic expansion since 1979 has been a carefully orchestrated, state-led affair. State-directed economic espionage has been a key part of this development strategy. From state-owned enterprises to state-championed industries, the PRC's economic development strategies don't just encourage cyber exploitation and technology transfer and acquisition, they *require it* to prime the pump of indigenous innovation. This openly acknowledged focus on technology acquisition, both licit and illicit, has resulted in the loss of hundreds of billions of dollars' worth of intellectual property from foreign firms and even more emphasis within the PRC on the value and efficacy of economic espionage as a means of economic development.

The Chinese House of Cards will Topple Without Growth

The PRC government views continued economic growth as a key means of maintaining power and control over the domestic population. For the most part, the Chinese population has demonstrated that they are willing to accept the ruling party and anti-democratic regulations so long as the economy grows. Achieving this spectacular yearly growth is a constant challenge. As China's economic growth slows, it is likely that Chinese technology acquisition will increase in an effort to stave off domestic instability or calls for political reform. The PRC has begun pushing towards redefining China as an innovation and higher-order manufacturing powerhouse, rather than the lowest-cost, lower-rung factory producer. A key part of this strategy is capitalizing on advanced technologies, whether stolen or indigenously developed, and creating products that can compete both domestically and internationally. Companies like Haier, Chinese smartphone maker Xiaomi, Lenovo, Huawei and Zhongxing Telecom (ZTE) are positioning themselves to aggressively compete globally with foreign firms, perhaps demonstrating the next wave of China's economic push. This presents a larger threat to foreign firms as they will now find themselves increasingly competing with joint venture partners who have co-opted their technologies and are now undercutting them globally.

China's Fascination with Duplication has a Strategic Purpose

Many people denigrate China for its fascination and proficiency at duplication, imitation and counterfeits, expressing exasperation and confusion as China copies things like the Eiffel Tower, brand name products and even entire European towns. However, Chinese expertise at copying should instead be viewed as a strategic decision designed to maximize economic growth. Why spend billions to research and develop something new that may or may not succeed when a Chinese firm can simply copy, and perhaps marginally improve upon, an existing product with existing demand and customer base?

Innovation is not a high economic priority for China. While Chinese firms are certainly capable of innovation, the cost benefit derived from espionage short circuits the need to expend resources in development that can better be spent in production. In other words, the emphasis on economic growth at all costs has resulted in less economic risk for Chinese firms that copy the intellectual property of others. Copying produces immediate financial rewards.

Top Ways the PRC acquires intellectual property/trade secrets

> **"There's only two types of corporations -- big corporations -- in America. Those who have been hacked by the Chinese, or those who don't yet know they've been hacked by the Chinese."**
>
> *- FBI Director James Comey*

The PRC's willingness to engage in state-sponsored and state-directed economic espionage takes many forms, but the threat from China doesn't simply come in the "how," but also in the "what."

In many industries, nearly anything related to a company's operations can be considered a target, particularly if the technology, goods or components will provide Chinese industry an economic advantage. The latest Chinese five-year economic plan (2011-2015) identified seven "national strategic emerging industries." These markets and others, including energy, aviation and automobiles, agriculture, pharmaceuticals and biotechnology, telecommunications, advanced materials development and higher-grade manufacturing, will likely see continued aggressive targeting. The following are illustrations of how Chinese trusted insiders have successfully spied on U.S. industry in recent years, and what technologies they have targeted.

Money for secrets

The Dupont Ring. The Pangang Group, a Chinese state-owned company, hired naturalized citizen Walter Liew to purchase trade secrets relating to the production of titanium dioxide (Titanium White) from an American engineer employed by Dupont. Liew convinced the engineer to make copies of over 400 pages of secret documents and provide photographs of restricted DuPont facilities. Liew and his wife were paid over $12 million by the Chinese which got access to the technology which was referred to as Dupont's most valuable trade secret in the world of paint.

The Seed Ring. "Inbred" or "parent" line seeds are valuable intellectual property. Inbred seeds are developed to have a particular trait (i.e. the Round-Up resistance), in order to cross breed with another inbred seed trait to develop a hybrid line of seed. Seed companies spend significant money in research and testing costs to develop success inbred lines of seed in order to develop hybrid seed. Mo Hailong, a Chinese Lawful Permanent Resident of the U.S. was the director of International Business for the Beijing Dabeinong Technology Company, part of the DBN Group, a leading Chinese agricultural science and technology conglomerate with a corn seed subsidiary that practices "patriotic agriculture." Mo lived in Florida, but made regular trips with several other individuals to specific fields and locations in Iowa and Illinois where they dug up corn seed from fields which were test-growing new lines of hybrid seed. Additionally, Mo purchased thousands of dollars' worth of corn seed from several seed dealers,

in cash over multiple years. Mo and his co-conspirators then attempted to covertly ship the seed to China. Mo also used an alias to visit the DuPont Pioneer headquarters and take a tour of a Monsanto research facility. Additionally Mo was seen visiting with a former Pioneer employee, now an executive with a Chinese seed company, whose wife still worked for Pioneer as a corn geneticist. The seeds targeted were reportedly worth $30-40 million and the goal was to obtain the benefit of U.S. companies' research and development without making the same investments.

Joint Venture stealing/technology acquisition

Sinovel Trade Secrets Ring. American Superconductor Corps (AMSC), formed a joint venture with Chinese state-owned company Sinovel Windtech to develop and build wind turbines in the Gobi Desert. Sinovel purchased software and equipment from AMSC for the wind turbines that Sinovel manufactured, sold and serviced. In March 2011, Sinovel owed AMSC over $100 million for products and services already delivered and entered into contracts to purchase over $700 million in future goods and services. However, Sinovel had no intention of continuing the relationship with AMSC and instead conspired to steal the source code and cut AMSC out. Sinovel recruited an AMSC engineer to secretly copy intellectual property from AMSC's computer systems, enabling Sinovel to copy the software, produce it under the company Guotong Electric, and cheat AMSC out of more than $800 million. After Sinovel successfully stole the software, it canceled its order with AMSC, causing AMSC's stock to lose 80% of its value and forcing the company to cut 150 jobs. Sinovel is looking to expand and market its stolen wind turbines globally.

Hiring away employees/Employee Moonlighting

Motorola. Motorola employee Jin Hanjuan was hired on the side by a Motorola competitor, Lemko Corp, and Chinese firm Sun Kaisens, which develops products for the Chinese military. The individual who hired Jin on the side was a former Motorola employee whose spouse was still employed by Motorola. Sun Kaisens gave Jin classified Chinese military documents to review as part of her work for them. Jin took two medical leaves of absence from Motorola, but retained her access to the Motorola servers, enabling her to download proprietary documents, including when she was in China. In February 2007, Jin left Motorola with over 1,000 documents containing technical information and marked confidential and proprietary which she attempted to take to China. Motorola estimates Jin stole roughly $600 million in corporate intellectual property.

NYU MRI Ring. Three men were working on a research grant from the National Institutes of Health at the New York University School of Medicine. NIH had awarded millions of dollars over five years to pay for Dr. Zhu Yudong's research into improving MRI technology. Simultaneously, the three men were receiving monetary support from Chinese companies, including a state-owned Chinese research institute. The men took bribes and other payments from a Chinese medical imaging company and the research center, in return for sharing nonpublic information

about their research. At the same time Zhu was leading research for the NIH, he was also leading a similar research project in China related to MRI technology that was funded by a grant from the Chinese government. Zhu also held a patent related to MRI technology, the value of which would be directly impacted by his grant research. In forms to NYU in connection with the NIH grant, Zhu falsely answered questions regarding outside affiliations and financial conflicts of interest. Zhu admitted to the FBI he had received nearly $500,000 in bribes for his work.

Industrial Espionage Cyber attacks

Unit 61398 Indictment. A Western District of Pennsylvania grand jury recently indicted five Chinese military officials for cyber crimes, including computer hacking and economic espionage. The indictment alleges that from 2006 until 2014, Chinese hackers from Unit 61398, a special unit of China's People's Liberation Army, stole technology that would provide a competitive advantage to Chinese competitor companies, including state-owned entities, from the following U.S. Companies: Westinghouse Electric Co., U.S. subsidiaries of SolarWorld AG, United States Steel Corp., Allegheny Technologies Inc., the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union and Alcoa Inc. The stolen information included trade secrets as well as confidential internal communications that would provide strategy insight information that could provide a competitive advantage to Chinese companies.

The sting operation against the Chinese hackers was a joint effort between the National Security Cyber Specialists' Network, a network of U.S. Attorney's Office prosecutors and other experts and the FBI. The FBI has placed the Shanghai-based soldiers on its Most Wanted list for over 31 counts including computer fraud, identity theft, economic espionage, and trade secret theft. The indictment describes a number of specific examples of how the hackers stole information, including the following:

- In 2010, while Westinghouse was building four power plants in China, a PLA hacker stole confidential and proprietary technical and design specifications for pipes, pipe supports, and pipe routing within the power plant buildings.
- In 2012, the hackers stole information about SolarWorld's cash flow, manufacturing metrics, production line information, costs, and privileged attorney-client communications relating to ongoing trade litigation and other issues.
- In 2010, while U.S. Steel was participating in trade discussions with Chinese steel companies, a PLA hacker sent spearphishing e-mails to U.S. Steel employees that resulted in the installation of malware on U.S. Steel computers.
- In 2012, while Allegheny Technologies was engaged in a joint venture with a Chinese state owned entity, PLA hackers gained access to Allegheny Technologies' network and stole network credentials for virtually every Allegheny Technologies employee.

- In 2012, while United Steel was involved in public disputes over Chinese trade practices, PLA hackers stole e-mails from senior United Steel employees containing sensitive, non-public information about United Steel strategies related to pending trade disputes.

- In 2008, three weeks after Alcoa announced a partnership with a Chinese state-owned entity PLA hackers sent spearphishing e-mails to Alcoa, which resulted in the theft of thousands of e-mail messages and attachments from Alcoa's computers.

Industrial espionage is the practice of stealing from a specific entity for the benefit of another. In these cases, Chinese PLA Unit 61398 specifically targeted information from U.S. companies that would provide an advantage to Chinese state-owned entities. When a foreign power uses military grade cyber-attacks to steal trade secrets from private companies, the result is a loss of innovation and investment in trade secrets. A company is simply less likely to put the time and effort into innovation, research and development if they suspect the Chinese will reap the rewards from their hard work.

How the Insider can thrive in your organization

"The Spy is in the Worst Possible Place"

- Robert Hanssen

While working undercover on the investigation to collect evidence against Robert Hanssen for espionage, Hanssen revealed to one of the authors of this White Paper what he called the central precept to any informed counterintelligence operation – that "the Spy is in the Worst Possible Place." Hanssen's explanation was that the spy is in the place where he is able to access those secrets that will create the most damage based on the spy's knowledge of who to provide those secrets to in order to make the most money for them. This cost benefit analysis of spying, straight from the mind of America's top spy, suggests that an insider relies on three critical points in order to spy successfully: (1) knowledge of relevant secrets that others want; (2) ability to access those secrets; and (3) understanding of where to sell the secrets for the maximum gain.

In Robert Hanssen's case, the spy most likely began his two-decade espionage career for financial gain. Indeed, when Hanssen explained what he called "Hanssen's Law" – that the spy is in the worst possible place – he had sketched his entire career as a spy. As a senior member of a counterintelligence unit focused on Russia, Hanssen had access to a wide variety of confidential internal information of significant value to the Soviet Union. As a trusted insider, he was able to access that information without creating suspicion. Finally, Hanssen's detailed knowledge of the Russian opposition's intelligence gathering practices provided Hanssen the perfect understanding of whom he should approach with the stolen information in order to put the most money in his pocket.

Snowden, on the other hand, *appears* to have acted because of an ideological stance that NSA's collection practices went above and beyond what was required to protect the interests of United States citizens (although this is subject to speculation). As a trained systems administrator with access to the NSA's systems, Snowden knew the release of the NSA information would create a massive media stir and draw intense attention on a world stage. As a trusted insider, Snowden had the capability to both collect information with his own access and to use social engineering (or trickery) to convince others to provide him their access. Finally, Snowden knew that providing the information to The Guardian Newspaper and potentially (and we must assume) intelligence agencies in China and Russia, would enable maximum exposure of the NSA's activities in order to damage the ability of the NSA to continue those practices into the future.

Financial gain in Hanssen's case and presumed ideology for Snowden are only two of the many reasons that an insider will spy. Generally, the basic motivations for committing espionage include money, ego, ideology, coercion or blackmail, and in more recent years, divided loyalties. These motivations are not mutually exclusive and most spies are motivated by more than one. However, what induces an otherwise loyal employee to turn is more art than science.

The exact qualities that are “flags” to security professionals can also be indicators of a top performer and someone worthy of promotion. The key to detecting the insider threat is having a real-time, collaborative program where all members of the community recognize their role in protecting the security.

Someone who engages in espionage, whether for a state or a commercial competitor, must have more than just a motivation to spy. Espionage requires an opportunity to betray, motivation to commit the crime, underlying character weaknesses and finally, a stressful trigger event to set things in motion. Common weaknesses include, but are not limited to, greed, impulsivity, narcissism, feelings of entitlement, an arrogant attitude that the rules only apply to others, vindictiveness, alienation, paranoia, naiveté and thrill-seeking. People who have these types of weaknesses are not guaranteed to spy, however individuals with these behavioral traits are at increased risk for maladaptive or counterproductive behavior in response to significantly stressful life events. Likewise, serious personal problems are not necessarily indicators of misconduct. It is the combination of these factors which can lead to an individual’s decision to commit espionage.

Insider threat has become an umbrella term which can encompass anything from a malicious or disgruntled employee to unintentional misuse of computer systems or poor security practices which allow data breaches or leakage. An insider can be an employee, a business partner, a contractor or anyone with authorized access.

For any company or national agency, the trusted insider represents the most dangerous threat. This is a person who, by virtue of their position, has the authorized access to authorized systems as a part of their daily duties but is using it to do unauthorized things. They know inside information and the secrets of the organization and are granted access to both physical locations and networks. They have access to and relationships with personnel at all levels of the organizations and know exactly how to cripple the organization or what keeps it afloat. They are the “spy in the worst possible place.”

The Importance of an Insider threat Program

> **"What is at stake is not just our government secrets but also the safety and security of our infrastructure, the intellectual property that underpins our future prosperity and the commercially sensitive information that is the lifeblood of our companies and corporations."**
>
> *- MI5 Director General Jonathan Evans*

Protecting a company's intellectual property has to be considered as important as the research and development that goes into it. Verizon's Data Breach Investigations Report for 2014 found that nearly 25% of cyber incidents were related to intellectual property theft.[1] Countries like France, Israel, Russia and India, as well as market competitors, also actively conduct economic espionage, however the volume of Chinese activity and broad variety of markets targeted, make China the most significant threat to a company's intellectual property and trade secrets. Creating and maintaining a robust security program is critical to maintaining profitability. American companies of all sizes are targeted and victimized and despite increased attention on cybercrime threats, organizations have made little progress in defending themselves.

Exact costs associated with insider threats or loss of intellectual property and trade secrets is difficult to determine because many companies choose not to report breaches. However according to the Commission on the Theft of American Intellectual Property, annual losses of U.S. intellectual property are estimated at over $300 billion. China accounts for 50-80% of the problem, depending on the industry.[2] And according to the Cybersecurity Watch Survey for 2013, 53% of surveyed companies experienced an insider incident, with the most common incidents being unintentional exposure of private or sensitive data; theft of intellectual property; unauthorized access to or use of information, systems or networks; and theft of other proprietary information, including customer records, financial records, etc.[3] The companies surveyed also articulated that although external actors committed the majority of electronic crime events, those perpetrated by insiders were more costly or damaging to the organization. According to a Cisco study, 11% of employees reported that they or fellow employees accessed unauthorized information and sold it for profit or stole computers.[4] And in the last four years, the FBI has doubled the number of trade secret arrests, with the vast majority of those prosecutions involving insiders.

---

[1] http://www.verizonenterprise.com/DBIR/2014/

[2] http://www.ipcommission.org

[3] http://www.cert.org/insider-threat/research/cybersecurity-watch-survey.cfm

[4] http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.html

Ten Key Ways an Organization Can Address the Insider threat:

1. Identify and compartmentalize your key information and technology. Know who has access to the critical information. Don't put all your eggs in one basket – its better to lose a piece of the puzzle than the entire picture.

2. Create and maintain a culture of accountability and security where IP protection is seen as everyone's responsibility. Set up an anonymous "hotline" for employees to report suspicious behaviors or concerns.

3. Ensure coordination and collaboration between HR, security, IT and the GC. Employee activities should be viewed holistically and every department (and employee) should see their role in protecting the company. The best asset in an organization is the employee that has the training, awareness and dedication to spot an issue and the courage to raise it to management.

4. Know your employees. According to CSO Magazine's 2012 CyberSecurity Watch Survey[5], organizations that experienced cybercrime perpetrated by an insider in the previous 12 months reported that 51% of the insiders violated IT security policies and 19% were flagged for behavior/performance issues.

5. Conduct training for managers on at-risk behavioral traits that indicate an increased likelihood of insider spying, including unreported foreign trips, seeking proprietary or classified information unrelated to work duties, paranoia about being investigated, and disproportionate anger over career disappointments. Managers should be able to recognize the most pertinent traits and "tells" indicative of a potential problem that requires professional outside review.

6. Review user accounts/remote access for sustained access needs and when employees are given notice of termination or are fired. Disable user accounts when necessary upon departure (or before) or while on long-term leave. CERT Insider Threat Center[6] determined that in more than 70% of IP theft cases, insiders stole the information within 30 days of announcing their resignation.

7. Implement and monitor audit technology. Watch for data exfiltration/anomalous downloads or printing. In our "employee moonlighting" example, Jin Hanjuan was using her remote access from China and while away from the company on medical leave. Additionally, she was downloading massive volumes of data from the internal network. With an auditing program, these activities could have been detected earlier or possibly prevented.

---

[5] http://www.cert.org/insider-threat/research/cybersecurity-watch-survey.cfm

[6] http://www.cert.org/insider-threat/research/index.cfm

8. Develop and maintain an awareness program. Employees should know there are programs in place to catch people and there are consequences. *See something, say something* is a campaign that has worked in a number of areas since the 9-11 attacks. The same sort of "open eyes" mentality where all employees are enlisted to protect company secrets is critical to catching the trusted insider.

9. Develop and maintain a program to monitor the internet and deep net for internal documents and technology.

10. Develop and maintain a business continuity program to maintain operations in the event a crisis strikes. Internal penetrations may be malicious and destructive, crashing servers and compromising the ability to carry out operations. A plan to keep the wheels turning at the same time the crisis is managed is critical to minimizing the damage.

How we can help

The Georgetown Group and **Castle Advisory Group** have teamed to bring a wealth of trusted insider investigative experience to our clients in an instructional and low impact manner. We have jointly developed a trusted insider program that takes a holistic look at an organization in order to conduct pinpointed investigations and research that highlights areas a company can strengthen to protect themselves. The following services are available upon request:

1. Develop and/or refine a **holistic insider threat program** for companies.

2. Conduct **training and education** for employees and management regarding insider threat awareness.

3. Conduct sensitive and confidential **vulnerability and threat assessments** to locate vulnerabilities and discover outside entities that may have targeted those vulnerabilities.

4. Conduct **due diligence** on potential partners, joint venture arrangements and other outside entities and conduct background investigations on current employees provided critical access to sensitive information and prospective employees, contractors and vendors.

5. Dedicated **investigative support** to internal investigations when a breach occurs.

6. **Cyber security vulnerability analysis** of your network and information control practices, a review of intellectual property and information protection policies and computer forensics and information systems monitoring.

7. Develop a **customized incident response strategy** that addresses not only the external hacking and social engineering risks, but addresses internal cyber vulnerabilities.

The Authors

Rachel Houhoulis is the Founder of **Castle Advisory Group** (www.castleadvisorygroup.com), a security and counterintelligence consulting firm with a focus on China. Ms. Houhoulis has nearly a decade of experience in the Intelligence Community serving as a Department of Defense subject matter expert on China counterintelligence issues, senior intelligence analyst for the Joint Chiefs of Staff China counterintelligence program, counterespionage investigator and conducting counterintelligence operations. She has consulted on many high-value investigations and intelligence operations and was a guest instructor at DoD's premier counterintelligence training academy and the Defense Academy for Credibility Assessments. She lived in China and speaks Mandarin Chinese.

Eric O'Neill is the founder of **The Georgetown Group LLC** (www.georgetowngroup.com), an investigative and security services firm. Mr. O'Neill is a practicing attorney who specializes in cyber security vulnerability assessments, counterintelligence and counterterrorism operations, investigations into economic espionage, internal investigations and security risk assessment consulting. Mr. O'Neill served as an operative for the FBI, where he conducted national security field operations against terrorists and foreign intelligence agents. His undercover role in the investigation and capture of the most notorious spy in United States history, Robert Phillip Hanssen, became the subject of Universal Studio's movie *Breach*, released to critical acclaim in 2007. Mr. O'Neill has broad legal experience in the areas of homeland security, border protection, risk and liability mitigation for anti-terrorism technologies, national security related matters and federal investigations of United States citizens and foreign nationals.

Mr. O'Neill is a professional speaker that is available to speak on the insider threat, cyber security, and numerous other security issues. For Mr. O'Neill's speaker bio, please visit www.ericoneill.net.

Eric M. O'Neill
The Georgetown Group LLC
www.georgetowngroup.com
202-656-9950
eoneill@georgetowngroup.com
1101 K Street, NW, #650
Washington, DC 20005

Rachel Houhoulis
Castle Advisory Group
www.castleadvisorygroup.com
571-721-1599
Rachel@CastleAdvisoryGroup.com

THE GEORGETOWNGROUP™
STATE OF THE ART INTELLIGENCE

Castle Advisory Group